FortiOS - Release Notes

Version 6.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

April 17, 2019
FortiOS 6.2.0 Release Notes
01-620-518032-20190417

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-03-28	Initial release.
2019-03-29	• Updated Upgrade Information > FortiClient Endpoint Telemetry license on page 24. • Added FortiAP-U and FortiAP-W2 to Product Integration and Support on page 28.
2019-03-29	• Added 526107 to Resolved Issues on page 33. • Updated Changes in default behavior > System > Devices configured under security-exempt-list are void after upgrading to 6.2.0. on page 9.
2019-04-01	• Added 548813 to Known Issues on page 53. • Added 487421 to Resolved Issues on page 33. • Updated FortiClient Endpoint Telemetry license on page 24.
2019-04-02	• Added the following notice: Device detection changes on page 23 • Added 540903 to Resolved Issues on page 33.
2019-04-03	Deleted 487421, 495090, 502940, and 510148 from Common Vulnerabilities and Exposures on page 52.
2019-04-08	Corrected bug number from 537289 to 538289 in Resolved Issues on page 33.
2019-04-15	Added the following special notice: NP4lite platforms on page 7.
2019-04-17	Removed *FortiAnalyzer units running older versions* from Special Notices on page 6.

Introduction and supported models

This guide provides release information for FortiOS 6.2.0 build 0866.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.0 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-POE, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-61E
FortiGate Rugged	FGR-30D, FGR-35D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCPONDEMAND
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.2.0 images are delivered on request and are not available on the Beta portal.

Special Notices

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

- FGR-30D
- FGR-35D
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E-2R
- FWF-50E
- FWF-51E

FortiGate hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D does not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

Changes in default behavior

Firewall

Remove dependency of `ssl-ssh-profile` on `utm-status` under firewall policy (531885).

Previous releases	6.2.0 release
You must enable `utm-status` under firewall policy before configuring `ssl-ssh-profile`.	You can configure `ssl-ssh-profile` by itself. When you upgrade, this configuration is added to the existing firewall policy.

Log & Report

Starting from the 6.2.0 release, `exe log list` displays the result of the current log device.

Previous releases	6.2.0 release
`exe log list` only lists the disk log file.	`exe log list` lists the log file from the current log device (disk/memory). `exe log list` shows the memory log file in `exe log filter device memory`. `exe log list` shows the disk log file in `exe log filter device disk`.

Separate policy and address `log-uuid` options into two individual options.

Previous releases	6.2.0 release

`config system global`
`  set log-uuid [policy-only | extended | disable]`
`end`
	`config system global`
	`  set log-uuid-policy [enable | disable]`
	`  set log-uuid-address [enable | disable]`
	`end`

System

Starting from the 6.2.0 release, Global admin can only back up but not restore the configuration file.

Previous releases	6.2.0 release
Super admin: can back up and restore configuration file. Global admin: can back up and restore configuration file. VDOM admin: can back up and restore VDOM configuration file with full Admin and Maintenance permission.	Super admin: can back up and restore configuration file. Global admin: can only back up configuration file. VDOM admin: can back up and restore VDOM configuration file with full Admin and Maintenance permission.

Devices configured under `security-exempt-list` are void after upgrading to 6.2.0.

FortiOS 6.2.0 removes any use of device enforcement from various FortiGate features.

Previous releases

```
config user device-category <--removed

config user device-access-list <--removed

config user device-group <--removed

config user security-exempt-list
   edit [List Name]
      config rule
         edit [Rule ID]
            set devices [Device or group
name] <--removed
            set srcaddr [Address or group
name]
         next
      end
   next
end

config system interface
   edit [Interface]
      set ip [IP address and subnet mask]
      set device-access-list [Access list
name] <--removed
      set device-identification-active-scan
[enable | disable] <--removed
   next
end

config firewall policy
```

6.2.0 release

```
config user security-exempt-list
   edit [List Name]
      config rule
         edit [Rule ID]
            set srcaddr [Address or group
name]
         next
      end
   next
end

config system interface
   edit [Interface]
      set ip [IP address and subnet mask]
   next
end

config firewall policy
   edit [Policy ID]
      set name [Policy name]
   next
end

config firewall policy6
   edit [Policy ID]
      set name [Policy name]
   next
end
```

Previous releases	6.2.0 release
edit [Policy ID] set name [Policy name] set device [Device or group name] <-- removed next end config firewall policy6 edit [Policy ID] set name [Policy name] set device [Device or group name] <-- removed next end	

Changes in CLI defaults

Anti-Spam

Rename `spamfilter` to `emailfilter`.

Previous releases	6.2.0 release
config spamfilter bwl end config spamfilter profile end config firewall policy edit [Policy ID] set spamfilter-profile [Profile Name] next end	config emailfilter bwl end config emailfilter profile end config firewall policy edit [Policy ID] set emailfilter-profile [Profile Name] next end

Data Leak Prevention

Rename DLP `fp-sensitivity` to `sensitivity`.

Previous releases	6.2.0 release
config dlp fp-sensitivity end	config dlp sensitivity end

Firewall

Rename `utm-inspection-mode` to `inspection-mode` under firewall policy.

Previous releases	6.2.0 release
config firewall policy edit [Policy ID] set utm-inspection-mode [proxy | flow] next end	config firewall policy edit [Policy ID] set inspection-mode [proxy | flow] next end

Add a new direction command to Internet service group. Members are filtered according to the direction selected. The direction of a group cannot be changed after it is set.

Previous releases	6.2.0 release
config firewall internet-service-group edit [Internet Service Group Name] set member 65537 65538 next end	config firewall internet-service-group edit [Internet Service Group Name] set direction [source | destination | both] set member 65537 65538 next end

FortiView

The following FortiView CLI has been changed in this release.

Previous releases	6.2.0 release
config system admin edit [User Name] config gui edit [Dashboard ID] config widget edit [Widget ID] set type fortiview set report-by source <- removed set timeframe realtime <- removed set sort-by "bytes" <- removed set visualization table <- removed next end next end next end	config system admin edit [User Name] config gui edit [Dashboard ID] config widget edit [Widget ID] set type fortiview set fortiview-type '' <- added set fortiview-sort-by '' <- added set fortiview-timeframe '' <- added set fortiview-visualization '' <- added set fortiview-device '' <- added next end next end next end

HA

The CLI command for HA member management is changed.

Previous releases	6.2.0 release
execute ha manage [ID]	execute ha manage [ID] [admin-username]

Intrusion Prevention

Move Botnet configuration option from interface level and policy level to IPS profile.

Previous releases	6.2.0 release
config system interface edit [Interface Name] set scan-botnet-connections [disable | block | monitor] next end config firewall policy edit [Policy ID] set scan-botnet-connections [disable | block | monitor] next end config firewall proxy-policy edit [Policy ID] set scan-botnet-connections [disable | block | monitor] next end config firewall interface-policy edit [Policy ID] set scan-botnet-connections [disable | block | monitor] next end config firewall sniffer edit [Policy ID] set scan-botnet-connections [disable | block | monitor] next end	config ips sensor edit [Sensor name] set scan-botnet-connections [disable | block | monitor] next end

IPsec VPN

Add `net-device` option under static/DDNS tunnel configuration.

Previous releases	6.2.0 release
config vpn ipsec phase1-interface edit [Tunnel Name] set type [static | ddns] next end	config vpn ipsec phase1-interface edit [Tunnel Name] set type [static | ddns] set net-device [enable | disable] next end

Log & Report

Move `botnet-connection` detection from malware to `log threat-weight`.

Previous releases	6.2.0 release
config log threat-weight config malware set botnet-connection [critical | high | medium | low | disable] end end	config log threat-weight set botnet-connection [critical | high | medium | low | disable] end

SDS.

Previous releases	6.2.0 release
config log threat-weight config malware set botnet-connection [critical | high | medium | low | disable] end end	config log threat-weight set botnet-connection [critical | high | medium | low | disable] end

Add new certificate verification option under FortiAnalyzer setting.

Previous releases	6.2.0 release
config log fortianalyzer setting set status enable set server [FortiAnalyzer IP address] end	config log fortianalyzer setting set status enable set server [FortiAnalyzer IP address] set certificate-verification [enable | disable] set serial [FortiAnalyzer Serial number] set access-config [enable | disable] end

Proxy

Move SSH redirect option from firewall `ssl-ssh-profile` to firewall policy.

Previous releases	6.2.0 release

config firewall ssl-ssh-profile
  edit [Profile Name]
  config ssh
  set ssh-policy-check [enable | disable]
  end
  next
end
	config firewall policy
	 edit [Policy ID]
	  set ssh-policy-redirect [enable | disable]
	 next
	end

Move HTTP redirect option from profile protocol option to firewall policy.

Previous releases	6.2.0 release

config firewall profile-protocol-option
  edit [Profile Name]
  config http
  set http-policy [enable | disable]
  end
  next
end
	config firewall policy
	 edit [Policy ID]
	  set http-policy-redirect [enable | disable]
	 next
	end

Move UTM inspection mode from VDOM setting/AV profile/webfilter profile/emailfilter profile/DLP sensor to firewall policy.

Previous releases	6.2.0 release

config system setting
  set inspection-mode [proxy | flow]
end
 	
config antivirus profile
  edit [Profile Name]
  set inspection-mode [proxy | flow-based]
  next
end
 	
config webfilter profile
  edit [Profile Name]
  set inspection-mode [proxy | flow-based]
	config firewall policy
	  edit [Policy ID]
	  set inspection-mode [flow | proxy]
	  next
	end

Previous releases	6.2.0 release
next end config spamfilter profile edit [Profile Name] set flow-based [enable | disable] next end config dlp sensor edit [Sensor Name] set flow-based [enable | disable] next end	

Routing

For compatibility with the API, the CLI command for OSPF MD5 is changed from a single line configuration to sub-table configuration.

Previous releases	6.2.0 release
config router ospf config ospf-interface edit [Interface Entry Name] set interface [Interface] set authentication md5 set md5-key [Key ID] [Key String Value] next end end	config router ospf config ospf-interface edit [Interface Entry Name] set interface [Interface] set authentication md5 config md5-keys edit [Key ID] set key-string [Key String Value] next end next end end

The name `internet-service-ctrl` and `internet-service-ctrl-group` is changed to `internet-service-app-ctrl` and `internet-service-app-ctrl-group` to specify it's using application control.

Previous releases	6.2.0 release
config system virtual-wan-link config service edit [Priority Rule ID] set internet-service enable set internet-service-ctrl [Application ID] set internet-service-ctrl-group [Group Name] next end end	config system virtual-wan-link config service edit [Priority Rule ID] set internet-service enable set internet-service-app-ctrl [Application ID] set internet-service-app-ctrl-group [Group Name] next end end

Add cost for each SD-WAN member so that in the SLA mode in a SD-WAN rule, if SLAs are met for each member, the selection is based on the cost.

Previous releases	6.2.0 release
config system virtual-wan-link config member edit [Sequence Number] next end end	config system virtual-wan-link config member edit [Sequence Number] set cost [Value] next end end

Add a load-balance mode for SD-WAN rule. When traffic matches this rule, this traffic should be distributed based on the LB algorithm.

Previous releases	6.2.0 release
config system virtual-wan-link config service edit [Priority Rule ID] set mode [auto | manual | priority | sla] next end end	config system virtual-wan-link config service edit [Priority Rule ID] set mode [auto | manual | priority | sla | load-balance] next end end

Security Fabric

Add control to collect private or public IP address in SDN connectors.

Previous releases	6.2.0 release
config firewall address edit [Address Name] set type dynamic set comment '' set visibility enable set associated-interface '' set sdn aws set filter "tag.Name=publicftp" next end	config firewall address edit [Address Name] set type dynamic set comment '' set visibility enable set associated-interface '' set sdn aws set filter "tag.Name=publicftp" set sdn-addr-type [private | public | all] next end

Add generic support for integrating ET products (FortiADC, FortiMail, FortiWeb, FortiDDoS, FortiWLC) with Security Fabric.

Previous releases	6.2.0 release
config system csf config fabric-device edit [Device Name] set device-ip [Device IP] set device-type fortimail set login [Login Name] set password [Login Password] next end end	config system csf config fabric-device edit [Device Name] set device-ip [Device IP] set https-port 443 set access-token [Device Access Token] next end end

Add support for multiple SDN connectors under dynamic firewall address.

Previous releases	6.2.0 release
config firewall address edit [Address Name] set type dynamic set color 2 set sdn azure set filter "location=NorthEurope" next end	config firewall address edit [Address Name] set type dynamic set color 2 set sdn [SDN connector instance] set filter "location=NorthEurope" next end

System

Add split VDOM mode configuration.

Previous releases	6.2.0 release
config global set vdom-admin [enable | disable] end	config global set vdom-admin [no-vdom | split-vdom | multi-vdom] end

WiFi Controller

Remove `http` and `telnet` in `allowaccess` options under `wireless-controller wtp-profile` and `wireless-controller wtp`.

Previous releases	6.2.0 release
config wireless-controller wtp-profile edit [WTP Profile Name] set allowaccess http | https | telnet | ssh next end config wireless-controller wtp edit [WTP ID] set override-allowaccess enable set allowaccess http | https | telnet | ssh next end	config wireless-controller wtp-profile edit [WTP Profile Name] set allowaccess https | ssh next end config wireless-controller wtp edit [WTP ID] set override-allowaccess enable set allowaccess https | ssh next end

Changes in default values

Firewall

The default profile for `ssl-ssh-profile` is changed from `certificate-inspection` to `no-inspection`.

Previous releases	6.2.0 release

Config firewall policy
  edit [Policy ID]
  set ssl-ssh-profile certificate-inspection
  next
end
	Config firewall policy
	  edit [Policy ID]
	  set ssl-ssh-profile no-inspection
	  next
	end

IPsec VPN

The default value for `net-device` option under dynamic(dialup) tunnel has changed from `disable` to `enable`.

Previous releases	6.2.0 release

config vpn ipsec phase1-interface
  edit [Tunnel Name]
  set type dynamic
  set net-device disable
  next
end
	config vpn ipsec phase1-interface
	  edit [Tunnel Name]
	  set type dynamic
	  set net-device enable
	  next
	end

Log & Report

The default value, minimum value, and maximum value for memory log is changed.

Previous releases	6.2.0 release

config log memory global-setting
  set max-size 65536
end
	config log memory global-setting
	  set max-size [1% of total RAM]
	end

Routing

The default SD-WAN `health-check` interval is changed from `1` to `500` and the unit is changed from `seconds` to `milliseconds`.

Previous releases	6.2.0 release
config system virtual-wan-link config health-check edit [Health Check Name] set interval 1 next end end	config system virtual-wan-link config health-check edit [Health Check Name] set interval 500 next end end

The default `link-monitor` interval is changed from `1` to `500` and the unit is changed from `seconds` to `milliseconds`.

Previous releases	6.2.0 release
config system link-monitor edit [Link Monitor Name] set interval 1 next end	config system link-monitor edit [Link Monitor Name] set interval 500 next end

System

The default protocol used for FortiGuard service communication is changed from UDP to HTTPS.

The protocol setting remains unchanged for FortiGates upgrading from v6.0 to v6.2.

Previous releases	6.2.0 release
config system fortiguard set protocol udp set port 8888 end	config system fortiguard set protocol https set port 8888 end

Switch Controller

The default value for FortiLink split interface is changed from `disable` to `enable`.

Previous releases	6.2.0 release
config system interface edit [FortiLink Interface] set fortilink enable set fortilink-split-interface disable next end	config system interface edit [FortiLink Interface] set fortilink enable set fortilink-split-interface enable next end

WiFi Controller

The default value of `broadcast-suppression` under wireless `vap` is changed from `dhcp-up arp-known` to `dhcp-up arp-known dhcp-ucast`.

Previous releases	6.2.0 release
config wireless-controller vap edit [vap-name] set broadcast-suppression dhcp-up arp-known next end	config wireless-controller vap edit [vap-name] set broadcast-suppression dhcp-up dhcp-ucast arp-known next end

The default value of `control-message-offload` under `wireless-controller wtp-profile` is changed from `ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu` to `ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health`.

Previous releases	6.2.0 release
config wireless-controller wtp-profile edit [FAP Profile Name] set control-message-offload ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu next end	config wireless-controller wtp-profile edit [FAP Profile Name] set control-message-offload ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health next end

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- Mac-address-based policies – A new address type is introduced (Mac Address Range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.2.0 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.0
- FortiClient EMS 6.2.0
- FortiClient 6.2.0
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.9 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.0. When Security Fabric is enabled in FortiOS 6.2.0, all FortiGate devices must be running FortiOS 6.2.0.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.0 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.0 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)

- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 6.2.0 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.0 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.0, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.0.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.0. FortiView widgets created in previous versions are deleted in the upgrade.

Product Integration and Support

The following table lists FortiOS 6.2.0 product integration and support information:

Web Browsers	• Microsoft Edge 41 • Mozilla Firefox version 59 • Google Chrome version 65 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 41 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 59 • Google Chrome version 65 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 24. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 24. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 24 and Fortinet Security Fabric upgrade on page 24. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later

FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later
FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0276 and later (needed for FSSO agent support OU in group filters) • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2008 R2 64-bit • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Novell eDirectory 8.8
FortiExtender	• 3.2.1
AV Engine	• 6.00127
IPS Engine	• 4.00219
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network: https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 61 Google Chrome version 68
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X El Capitan 10.11.1	Apple Safari version 11 Mozilla Firefox version 61 Google Chrome version 68
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 6.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Anti-Spam

Bug ID	Description
295539	Spam filter profile CLI options are disabled after GUI change.
477496	Unable to add email wildcard to black/white list GUI in Anti-Spam profile.

AntiVirus

Bug ID	Description
474538	Remove mobile malware protection option from GUI.
491675	FTP Server is not accessible when AV profile is set to proxy based inspection.
502138	AV full-scan mode causes traffic to fail.
513667	WAD crash when `av-scan` is blocking the input and HTTP session is closing.
516072	In flow mode, scanunit API does not allow IPS to submit a scan job for a URL with no filename.
519759	Process scanunit crash in `removeTransformCleanup` when Outbreak Prevention is enabled.
522343	`scanunitd` experiences a constant different kind of crash.
525151	Flow AV profile and SSL deep inspection writes blocked invalid cert logs to webfilter logs.
525711	FortiGate not sending email headers to FortiSandbox.
537666	Flow AV in quick mode cannot block large infected samples (`eicar.exe`).
541023	Scanunit worker leaves urlfilter API socket files behind in tmp.

Application Control

Bug ID	Description
511151	Application Control with traffic shaper is not attached to session.

Authentication

Bug ID	Description
447575	Standard vs. Advanced mismatch on FortiOS GUI.

Bug ID	Description
463849	FAC remote LDAP user authentication via RADIUS fails on invalid token if password change and 2FA are both required.

Data Leak Prevention

Bug ID	Description
486958	`scanunit` signal 14 alarm clock caused by DLP scanning bz2 file.
496255	Some XML-based MS Office files are recognized as ZIP files.
518146	DLP incorrectly blocking .deb file extension (DLP log unclear for matches in archive files).
524910	DLP profile to block the file name pattern "*" not blocking uploading files.

DNS Filter

Bug ID	Description
472267	DNS filter performance improvement.

Endpoint Control

Bug ID	Description
543635	Extend GTP0/GTP1 policy for new RAT types.

Explicit Proxy

Bug ID	Description
413187	XFF header enhancements (strip-off & enforcement) for URL filtering module.
445312	`tcp-timewait-timer` does not have any effect when WAD is running.
477289	Proxy is unexpectedly sending FIN packet (FTP over HTTP traffic).
491118	Kerberos users unable to access the internet.
500182	UDP over SOCKS PROXY.
503478	Presence of X-XSS-Protection header causes response to be not cacheable.
506654	High memory usage on WAD.
506821	Explicit web proxy, slow speed.
509876	Web-proxy internet service as DST address cannot work for some IP address range overlap case.
509994	Website denied due to certificate error (revoked) only in Proxy_policy and deep inspection profile.
512294	WAD should not keep buffer data if the server's response broke the HTTP protocol.

Bug ID	Description
515327	WAD returns *502 Bad Gateway* if the server disconnects without data received.
521344	Explicit FTP proxy doesn't work with second IP address.
521899	When proxy srvc is set to protocol CONNECT and client tries to connect to HTTPS page, client gets message: Access Denied.
524933	Agentless NTLM - FortiGate adds redundant domain suffix to username when it is already present (UPN used).

Firewall

Bug ID	Description
390422	Cannot add a wildcard FQDN object to an addrgrp which is applying in policy
457294	GUI to allow negate an address object.
466999	Implicit deny policy generating logs when logging is disabled.
484599	Cannot use custom internet service group in traffic shaping policy.
484603	Cannot use application group in traffic shaping policy.
492034	Traffic not matching expected sessions and getting denied.
497535	In NGFW policy mode, applications allowed by unintended policy ID when together with `firewall-session-dirty check new`.
503904	Creating a new address group gives error: `Associated Interface conflict detected!`.
508085	Customer does not accept the confirmation of 0.0.0.0/0 object while creating address object errors.
508098	Creating wildcard address object errors but still creates the object.
511143	`set logtraffic-start enable` option is not available for `policy64/policy46`.
520558	Should not do passive port NAT for FTP session helper.
521337	Adding ports in a custom ISDB service for all the IP of the service is not easily achievable.
522447	FortiGate logging is not stable and stopped working.
525995	Session marked dirty when routing table updated for route which is not related to the session.
529685	WCCP not use the tunnel.
535468	DCE/RPC session-helper expectation session is removed unexpectedly.
536868	A FortiGate in TP mode with set send-deny-packet enabled policy, generates strange ICMP-REPLY for TCP SYN/ICMP-REQUEST/UD.
537227	When forwarding the multicast traffic for the first time, the packet size is not calculated correctly.
541248	FortiGate does not offer `TLS-RSA-*` ciphers when virtual server is configured and `strong-crypto` is disabled.
541596	Virtual server rejects TLS connections when plain RSA ciphers are specified in custom cipher-list.

FortiView

Bug ID	Description
256264	Realtime session list cannot show IPv6 session and related issues.
414172	HTTPsd / DNSproxy / high CPU / memory with high rate UDP 1Byte spoofing traffic.
453610	*Fortiview >Policies(or Sources) >Now*, it shows nothing when filtered by physical interface at PPPoE mode.
460016	In *Fortiview* > *Threats*, drill down one level, click *Return* and the graph is cleared.
488886	*FortiView* > *Sources* is unable to sort information accurately when filtering by policy ID number.
521497	*FortiView* > *All Sessions* > *real time view* is missing right-click menu to end session/ban ip.
527751	No user name on *Fortiview* > *Sources* main page

GUI

Bug ID	Description
457966	Virtual wire pair > Add VLAN range filter on GUI.
462011	GUI is blank when accessed by radius user with read-access profile.
469082	`prof_admin` profile admins not able to display GUI IPv4 source address.
470698	Create new default dashboards in factory default settings.
473148	FGT5001D Sessions widget in Dashboard show negative % for nTurbo after throughput test.
478057	Cannot restore configuration when GUI access to the FortiGate is via a connection with small bandwidth.
493704	While accessing FortiGate page, browser memory usage keeps spiking and finally PC hangs.
498738	GUI creating B/W widget referencing SIT-Tunnel generates error.
501911	In FOS-AWS prompts user password = instance ID, and forces user to change password upon initial log in.
502785	Remove *# of interfaces* from device list.
503867	Some certificates break Certificate page.
505187	Getting error *Some changes failed to save* when configuring IPv4 policies on firewall.
509791	Editing Address Objects name within SSL-SSH inspection profile selection pane cause loss of Address/Web exemption objects.
509978	Unable to download the results of the scheduled script.
515022	FortiGate and FSA has right connectivity, but Test Connectivity on GUI interface is showing `Unreachable or not Authorized`.
516295	*Error connecting to FortiCloud* message while trying to access Forticloud Reports in GUI.

Bug ID	Description
518964	Slowness when adding or removing member from address group via SSH.
518970	Suggestion to improve SD-WAN SLA creation page's invalid-entry handling.
521253	LAG interface is not listed on the dropdown list when configuring DNS Service.
523902	REST API issue: Access Token only verifies the first 30 characters.
526748	Firewall policies with action DENY show default proxy-options applied in GUI.
527137	Local GW disappears from GUI.
528464	Disappearing policy add-also happens in 6.0.3 build 0200.
533018	Process `nsm` with high CPU when displaying the GUI section of IP4 and IPv6 policy when receiving full routing of BGP.
536841	DNS server in VPN SSL setting is overwritten when SSL-VPN settings are modified via GUI.

HA

Bug ID	Description
445214	Slave in AP cluster memory/CPU spike as a result of DHCP/HA sync issue.
461915	When *standalone config sync* is enabled in FGSP, IPv6 setting of interface is synced.
477392	Can't use FAC username, password, and FortiToken two-factor authenticate login HA slave unit.
481943	A green check mark indicating HA sync status on GUI is only put on a side of virtual cluster 1.
482548	Conserve mode caused by hasync consuming most available memory.
486846	FGSP session sync for FGCP cluster keeps syncronizing sessions back to the originator even after the traffic is stopped.
487444	FortiGate stops accepting traffic from any interface in a hardware switch after HA fail-over in 80/81E.
494029	After failover, cannot connect to management-IP of backup device.
503433	`hasync` daemon crashes when admin session timeout and cluster could be out of sync for a short period.
503763	Config sync communication on heartbeat link not encrypted when encryption is enabled under system HA.
503897	FG-501E units generating logs only for five minutes after rebooting the unit, then do not generate anymore logs.
507013	Out of sync after config change.
509557	Duplicate MAC on mgmt2 ports.
510660	Upgrade to build 3574 fails for HA cluster.
511522	HA uninterruptible upgrade from 9790 to 3558 fails.

Bug ID	Description
513940	Enormous amount of session between heartbeat Interfaces for port 703 (HASYNC).
515401	SLBC-Dual mode: Slave chassis blade sending traffic logs.
516234	GUI checksums show slave is not synchronized when the master is synchronized.
517537	Slave out-of-sync. Unable to log into slave unit.
518116	Suggest to add a command to show virtual_mac usages on FGCP HA.
518621	`ha-mgmt-interface` IPv6 GW is not registered when `ha-mgmt-interface` IPv4 GW is **not** set.
518717	MTU of session-sync-dev does not come into effect.
519653	Increase FGSP session sync from 200 VDOM to 500 VDOM.
523733	Successive failovers lead to complete traffic stop (IPSEC[01]_IQUEUE counter catching all traffic).
526252	High memory caused by updated daemon.
526492	FGSP between two FGCP clusters - session expectation.
526703	FGSP of FGCP cluster, does not pickup NAT'ed sessions.
530215	Application `hasync *** signal 11 (Segmentation fault) received ***`.
531083	Config of HA pair of FortiGates goes out of sync when removed from Central Management (FortiManager).
531812	FGSP config replicating BGP and OSPF info after a config restore.
532015	High CPU on Core1 due to session sync process.
535534	Multicast-forward setting is lost after a backup restore on a FGCP cluster.
538289	Old master keeps forwarding traffic after failover.
539707	Wrong status for ping server after failover in the output of the command `get sys ha status`.

ICAP

Bug ID	Description
478617	ICAP X-Authenticated-Groups information.

Intrusion Prevention

Bug ID	Description
381062	Provide accurate statistics across multiple IPS daemons.
452131	`ipsengine` up time on FG-51E is a negative number after changing db from extended to regular.
469608	ICMP Packets drop while FGD updates.

Bug ID	Description
476219	Delay for BFD in IPinIP traffic hitting policy with IPS while IPsec calculates new key.
489557	`traceroute` issues when IPS is enabled.
503895	Traffic drops for 15 seconds when UTM is enabled.
509352	`IPv4.Invalid.Datagram.Size` attack is not detected in IDS mode.
516128	Victim is quarantined after IPS attack.
517059	One arm sniffer is unable to see HTTPS log in web filter logs.
537162	High memory due to IPS and SSL-VPN going into conserve mode.
541224	Network loop over virtual-wire-pair in HA mode if running diagnose `sys ha reset-uptime`.

IPsec VPN

Bug ID	Description
463441	NAT -T broken with AWS and Fortigate.
471326	AES-256-GCM for phase 1.
481720	Using transparent mode and policy base VPN, about 4 ICMP packets which exceed over MTU 1375 byte are dropped.
491305	Packet from FCT can not go through VXLAN over IPsec depending on packet size.
493918	Memory leak with IKED.
494285	Slow IPsec traffic between FortiGate and AWS FortiGate once run iPerf between unix and linux.
509559	`Invalid ESP packet detected (replayed packet)` when having high load on IPsec tunnel.
514519	OSPF neighbor can't up because IPsec tunnel interface MTU keeps changing.
515132	ADVPN shortcut continuously flapping.
515375	VPN goes down randomly, also affects remote sites dialup.
517088	IPsec Gateway never clears unless manually forced.
517849	Index of existing OIDs changes when installing new IPsec tunnels to the FortiGate - breaks monitoring.
518063	DPD shows unnegotiated and is not functioning correctly on ADVPN Spoke.
519187	IKE route should not be deleted if it is needed by other `proxyids`.
520151	When two certificates are configured on p1, both aren't offered or the wrong one is offered.
523567	MTU values does not gets calculated correctly in GRE over IPsec.
524101	Unnecessary next-hop restriction on static route prevents using static routing on Hub with 'net-device disable.'

Bug ID	Description
527496	Rename One Click VPN to Overlay Controller VPN.
529448	Shouldn't `PPK:no` be shown at IKEv2 SA level when `NO-PPK-AUTH` was used?
531203	Cannot edit existing phase1-interface config.
536899	One issue and two possible enhancements when proxying IKE mode-cfg and DHCP.
537140	KEv2 EAP - FortiGate fails to respond to IKE_AUTH when ECDSA certificate is used by ForitGate.
537450	Site-to-site VPN policy based - with DDNS destination fail to connect.
537769	FortiGate sends failure response to L2TP CHAP authentication attempt before checking it against RADIUS server.
537848	FortiGate IPsec VPN phase1-interface and phase2-interface configurations are not saved into configuration file.
540560	Missing IKE SA HA sync when FortiGate is mode-cfg client + xauth.

Log & Report

Bug ID	Description
387324	Archive mark is always on under UTM logs page when log-display location set to FAZ.
477393	Negative values in 'Load Balance' monitor logs.
479607	Scheduled auto-update happens twice in ten seconds but a log entry for the first try is not logged.
490379	Long-live session statistics logs add `sentdelta` and `rcvddelta` fields for FortiCloud FortiView as required.
491914	`miglogd : syslog` reliable mode is claiming all logs failed when some pass.
503394	Duplicate description for different log IDs: LOG_ID_CHG_CONFIG & LOG_ID_CONF_CHG etc.
503395	Duplicate description for different log IDs: LOG_ID_POWER_FAILURE, LOG_ID_POWER_FAILURE_WARNING etc.
503396	Duplicate description for different log IDs.
503397	IPsec logging - Duplicate description for different log IDs.
503398	AP Event log: Duplicate description for different log IDs.
503399	PPPOE Event log: Duplicate description for different log IDs.
503400	RADIUS event log: Duplicate description for different log IDs.
503401	SSL Event logs: Duplicate description for different log IDs.
504012	Duplicate description for different log IDs: LOG_ID_LEAVE_FD_CONSERVE_MODE, LOG_ID_LEAVE_FD_CONSERVE_MODE_NOTIF.
505393	Quad File Dropped Reason *forticloud-daily-quota-exceeded*.
510973	FortiGate with disk and send logs to FAZ has PCI alerts.

Bug ID	Description
518402	`miglogd` crash and no logs are generated.
521020	VPN usage duration days in local report is not correct.
523829	When destination interface is PPPoE, intf-role is logged as *Undefined* even though the role is not undefined.
540157	Cannot view logs from FortiGate when secondary IP is used (only secondary IP is allowed to go internet on upstream).
540903	Missed filename in the office365_Attachment. Download DLP log while it is blocked\Allowed.

Proxy

Bug ID	Description
458057	Constant DNS query on built-in FQDN cause network congestion.
470407	IPv6-Happy-Eyeballs-Mechanism not working with proxy-based Webfilter-Profile.
487096	SSL handshake fail when activate ESET application.
491417	FortiGate is dropping server hello packets when urlfilter is enabled.
492372	Multiple WAD crashes with signal 11 (Segmentation fault).
500965	FGT-200E in kernel conserve mode. WAD process consuming high memory.
505171	ICAP does not work if there is no other proxy-based UTM feature enabled in the policy.
506995	FGT1200D WAD Crashing 5.6.5 (wad mapi).
507155	System went into conserve mode due to wad after upgrade to 5.6.5.
507585	Support multiple DC servers in the agentless NTLM auth as well as user based matching.
512434	Need to do changes in default replacement message of `Invalid certificate Message`.
512936	SSL certificate inspection in proxy mode doesn't use CN from Valid Certificate for categorization when SNI is not present.
513270	Certificate error with SSL deep inspection.
516147	WAD crashes.
516863	Webproxy learn-client-ip webfilter's auth/warn/ovrd does not work.
518933	Certificate inspection (CN base) web category filter doesn't work.
519021	The customer is unable to access internal CRM application server with antivirus enabled.
521051	HTTP WebSocket 101 switching protocol requests mismatch in v6.0.3.
525518	Skype call drops when handled by WAD process after around three sec of being answered.
526322	WAD Crashes when processing transparent proxy traffic after upgrade to 6.0.3.
526667	FortiGate doesn't forward `request:port` command after 0 byte file transmission.

Bug ID	Description
529792	WAD process crash with signal 11.
530906	Certificate chaining is broken on FortiGate site (deep inspection) for certain web sites.
531526	FTP proxy ignores OTP in authentication.
531575	Web site access failure due to OCSP check in WAD + Deep SSL inspection.
532121	WAD uses high CPU with "netlink recvmsg No buffer space available" after upgrade to 6.0.3+.
534346	WAD memory leak on OCSP certificate caching.
536063	SSL deep inspection doesn't work with OCSP stapling.
536623	WAD performs category SSL-Exemptions when SSL-inspection profiles are in "protect-server" mode.
537183	Removed default `ssl-exempt` entries page show empty.
539452	FortiGate does not follow Authority key identifier when sending certificate chain in deep inspection.
540067	Wildcard addresses removed from SSL deep inspection exempt list after upgrade to 6.0.4 from 5.6.

REST API

Bug ID	Description
424403	REST API for system csf didn't return csf group name.
467747	REST API user cannot create API user via autoscript upload and cannot set API password via CLI.

Routing

Bug ID	Description
441506	BGP Aggregate address results in blackhole for incoming traffic.
448205	Network devices must be configured with rotating keys used for authenticating IGP peers that have a duration of 180 days or less.
449010	WAN LLB session log `srcip` and `dstip` are mixed up intermittently.
476805	FortiGate delays to send keepalive which causes neighbor's hold down timer to expire and reset the BGP neighborship.
485408	Merge vwl_valeo project - No option for proute based on only dynamic routes.
499328	Add VRF filtering capability to command `get router info routing-table all`.
500432	IGMP multicast joins taking very long time and uses high NSM CPU utilization.
503638	*config system ipip-tunnel* is lost after reboot when pppoe interface is used.
505189	Kernel is missing routes.
509561	SD-WAN health check status log is incorrect.

Bug ID	Description
509768	Spillover rules do not work on PPPoE virtual-wan-link.
511203	When using policy route for IPv6, NAT64 does not work.
511932	Can't make mgmt1 and mgmt2 redundant interfaces.
515683	FortiGate generates fragmented OSPFv3 DBD packets.
518655	IPv6 doesn't respond to neighbor solicitation request.
518677	Log message `MOB-L2-UNTRUST:311 not found in the list!` seen on VDOM with IPv6 router advertisement enabled.
518943	RIPv2 with MD5 authentication key ID incompatible with other vendors.
519498	Cease unspecified sent to all BGP peers when new peer is created.
522258	Some missing fields in `proute` list.
522271	Central NAT - Not updating when dst interface changes.
525182	WLAN guest user in VDOM makes the cluster out of sync.
526008	Differences between routing table and kernel forward information. ADVPN + BGP.
527478	Proute list fill "null " application name.
529683	Upgrade from 5.6 to 6.0 causes all routes to be advertised in BGP.
530545	SD-WAN Health-Check - Reported packet loss inaccurate.
531660	With VRRP use VRDST checking without default gateway.
531947	SD WAN IPsec interfaces keep failing over when link selection strategy is set to Custom-profile.
532257	OSPFD crash (Segmentation fault) - NSSA - removal of network statement for interface in 'down' state.
537110	BGP/BFD packets marked as CS0.
538411	Successfully configured static route CLI commands fail with parse errors after reboot.
539982	Multicast failed after failover from another interface.
540103	OSPF6 will advertise only /128 prefixes to neighbours using point-to-point network type.
544603	Multicast on interfaces with secondary IP addresses.

Security Fabric

Bug ID	Description
473086	Quarantine monitor, should support showing devices for the whole fabric.
481381	Industry field shows up abnormally when adding security rating widget.
491508	If downstream device is part of security fabric, it should be exempted from FortiClient enforcement.

Bug ID	Description
504773	Some minor GUI improvement to facilitate security fabric config.
505068	Add CSF trust-list support into GUI.
505073	Should let *approval request* message be more standing out.
505656	Edge: Page reloaded when hovering on a connecting line between objects in topology.
525790	Not able to connect through SSL VPN to addresses resolved by SDN dynamic objects.
537130	Email notifications from automation stitches are being sent with a blank from field.

SSL VPN

Bug ID	Description
453740	Remove unused java source file in fortiweb/java.
466438	High CPU usage by sslvpnd [web and mixed mode].
477231	Unable to login to VMware vSphere vCenter 6.5 through SSL VPN web portal.
482497	Running *diagnose npu np6lite session* in FGT-201E results in high CPU and system instability.
483712	SSLVPND consumes high memory causing FGT enter conserve mode.
491130	SSLVPND 100% VPN when accessing OWA through bookmark.
491733	SSL VPN process taking 99% of CPU utilization even not using SSL VPN.
492654	SSLVPND process is crashing and users are disconnecting from SSL VPN.
493127	Connection to web server freezes when using SSL VPN web bookmark.
496584	SSL VPN bad password attempt causes excessive bindRequests against LDAP and lockout of accounts.
500901	SSL VPN web portal connect to FMG (5.6.3) unable to view Managed devices and policy packages.
508101	HTTPS bookmark to internal website produces error after the initial successful login.
509333	SSL VPN to Nextcloud doesn't open.
511107	RADIUS 2FA + password change against FAC fails due to unexpected state AVP + GUI bug.
511111	When accessing an internal listing website via SSL VPN, loading long lists fails or is interrupted.
515370	SSL VPN access denied if address object added after group object in firewall policy
517819	Unable to load web page in SSL VPN web mode.
518406	Unable to load WebPage through SSL VPN webmode. Some js files of xunta internal web sites have problems.
519113	SSL VPN web mode SMB connection doesn't work when enable then disable SMBCD debug.
519483	*Invalid HTTP Request*' when SMB via SSL VPN bookmark is executed.

Bug ID	Description
519987	HTTP bookmark error `SyntaxError: Expected ')'` after accessing internal server.
520307	Unable to view Cisco APIC web interface page after logging using SSL VPN web portal.
520361	SSL VPN portal not loading predefined bookmarks.
520965	IBM QRadar page not displaying in SSL VPN web-mode.
521459	HSTS header missing again under SSL VPN.
522987	Backup and restore the VDOM config with SSL VPN settings causes some critical flags and counter for SSL VPN to not update so SSL VPN stops working.
523450	Unable to access internal website via bookmark in SSL VPN web mode.
523647	Search result gives empty output upon accessing the URL *https://ieeexplore.ieee.org* via SSL VPN bookmark.
523717	Dropdown list can not get expanded through bookmarks (SSL VPN).
525106	HTML PABX Admin Console not working correctly in SSL VPN Mode.
525375	Atlassian Confluence wiki Javascript problem via SSL VPN web mode.
527342	sslConnGotoNextState:298 error when use SSL VPN bookmark method access huawei appliances.
527348	JavaScript script is not available when connecting using SSL VPN web mode.
527476	Update from web mode fails for SharePoint page using MS NLB.
528289	SSL VPN crashes when it receives HTTP request with header "X-Forwarded-For" because of the wrong use of `sslvpn_ap_pstrcat`.
528630	For SSL VPN with the realm named `sslvpn`, the authentication fails.
529186	Problem loading reaching internal web server through SSL VPN Web bookmark when using HTTPS. Some js files of "srvdnsmgt" do not run correctly.
529930	Scrolling in Jira is not working in SSL VPN web mode.
530223	SSL VPN wants client certificate even when no client-cert for realm is configured.
530833	Synology NAS login page stuck after login when accessing by SSL VPN Web portal.
531683	Can't authenticate on internal web server using web mode SSL VPN.
531827	Active cache memory leak after upgrade to 6.0.3 GA.
532261	SSL VPN web mode RDP connection not working when security set to NLA.
532464	Unable to load webpage in SSL VPN Webmode.
533008	SSL web mode is not modifying links on certain web pages.
534728	Unable to get dropdown menu from internal server via SSL VPN web mode connection.
535739	SSL VPN bookmark fails with JavaScript error.
536058	Redirected port is not entered in the URL through SSL VPN web mode.

Bug ID	Description
536847	Not able to access OnlyOffice through SSL VPN web mode.
537120	Adding latest macOS in the SSL OS-check-list.
537133	SSL VPN web mode gets redirected out of SSL VPN proxy.
537275	SSL VPN for users with passwords that expires allows password change after the password is expired.
537341	SSL bookmark is not loading a SAP portal information.
538904	Unable to receive SSL tunnel IP address.
539187	SSL VPN random stale sessions exhausting IP pool.
539948	Unable to load webpage in SSL VPN web mode.
545492	Unable to change tabs for internal website through web SSL VPN HTTPS bookmark.

Switch Controller

Bug ID	Description
306406	FortiSwitch Ports page display improvements.
503402	Switch controller event: duplicate description for different log IDs.
512112	Add `allowaccess` profile to the physical interfaces on the FortiSwitch.
522457	After a physical port of FortiLink LAG has link down/up, `fortilinkd` packet cannot be sent from FortiGate to FortiSwitch.
527521	On FortiSwitch Ports page, Display More does not work.
529915	FortiGate sends FortiSwitch serial# in SNMP trap fgFcSwName instead of FortiSwitch hostname.
530237	HA cluster out-of-sync after changing port POE mode on switch-controller managed-switch settings : Double commit.

System

Bug ID	Description
370151	CPU doesn't remove dirty flag when returns session back to NP6.
404944	Kernel Panic on creation of aggregate interface belonging to different NP6, when NP6 is configured in low latency mode.
408977	802.1AX L4 algorithm and NP4 do not distribute UDP evenly on egress LAG bundle.
415910	CPU cores utilization shows 0 percent while handling CPS in 5.4.
435910	On FG-50E and FG-51E ifHCOutOctets rolls as if counter32.
462178	Front Panel "SPEED" LED is flushing Green when Transmitting & receiving data.

Bug ID	Description
466805	Adding USB Host devices to a virtual machine connected by USB to FortiGate 500D causes the units to restart in loop.
468684	EHP drop improvement for units using NP_SERVICE_MODULE.
471191	Request to improve CLI help text for config system NP6 session-timeout options.
474737	*fwgrp* read&read-write access profile doesn't work properly.
477886	PRP support.
479533	`skippingBad tar header` message flooding on console after rebooting box and retrieving logs.
481511	Sniffer packet feature does not display any reverse packets on trunk interface.
482916	WAD crash with signal 6.
488400	FGFM sessions timeout when NPU offloaded (also applies to 6.0.0).
489772	`vlan-filter` is not straightforward.
491425	FortiGate sends MAB packet two minutes after receiving Access-Reject.
492441	Policy packet capture does not show timestamp.
492655	DNSproxy does not seem to update link-monitor module.
493126	One of the aggregate port members is transmitting irregularly LACP packets.
495572	Some of the FortiGate SNMP OIDs not giving any value.
496934	DNS Domain List.
498636	External resource should not update CMDB and cause FortiManager revision.
499435	Allow packet sniffer to use RAM disk.
503318	Accessing FDS via proxy server without DNS resolution.
504057	Service Object Limitation of 4096 needs to be increased.
505252	EMAC VLAN: SNMP data is incorrect.
505468	Incorrect SNMP answer for `get-next`.
505522	Intermittent failure of DHCP address assignment.
505715	DHCP lease new IP to same EFTPOS S800 device cause DHCP lease exhausted.
505927	ddnscd fortiddns monitor-interface is not being updated properly.
505930	FG3700D freeze when deleting VDOM.
506223	FortiGate is not compliant with rfc3397 (Domain Search Option Format).
507518	Partial configuration loss after root VDOM restore.

Bug ID	Description
509939	Firewall objects not visible or editable (Return code -361) when logged in via SSH key authentication.
510200	FGT DNS configuration doesn't allow one word domain names.
510419	HTTP link-monitor - response parser is case-sensitive (Content-Length header).
511018	SSH/SSL VPN connection to external VLAN interface drop by changing unrelated interface IP or restart OSPF.
513339	Finisar FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL transceivers not detected by FortiOS.
513419	High CPU on some cores of CPU & packet drops around 2-3%.
516783	DSA and RSA fingerprints are identical.
519246	`ipmc_sensord` process not checking sensors due to pending jobs.
519492	Not able to access TP FortiGate from different network.
519493	MCLAG: if remote side change systemID, only one port goes down, the other remains up.
521193	DNSPROXY causing high CPU usage.
521902	Addresses are taking a long time to load.
524083	MSS size negotiation is wrong when configured MTU value is less than 297.
524422	Merge br_6-0_sp back to 6.0 and 6.2.
525813	FortiGate managed by FortiManager intermittently going offline after rebooting FortiGate.
526240	Inactive interfaces in LAG causing unbalance packet distribution and link saturation.
526646	LAG interface flaps when the member ports go up.
526771	Allow sit-tunnel to not specify the source address.
526788	Password policy forces password change even if expire-status is disabled.
527390	Kernel panic in the HA cluster with FortiGate-3800D units running FortiOS v6.0.0 build 0200
527599	Internal prioritization of OSPF/BGP/BFD packets in conjunction with HPE feature.
527902	TXT records are truncated in DNS replies, when FortiGate is used as DNS server.
528004	Add global log device statistics to SNMP.
528465	GRE tunnel does not come up.
531584	Kernel Panic when Fragmented Multicast Traffic received on EMAC-VLAN interface.
531636	Certificate chain validation fails when trying to fetch the intermediate CA cert; untrusted cert presented.
532966	In SNMPv3 config, to select the Encryption Algorithm should be "Encryption Algorithm" instead of the label "Authentication Algorithm".

Bug ID	Description
533556	Read-only admin account can delete IPsec SA.
535420	SNMPv3 traps settings are not available in the GUI.
535730	Memory leak after upgrade to 6.0.4.
536520	GTP Tunnel States are not synced on subordinate unit after a reboot.
536817	FortiGate sending DHCP offer using broadcast.
539090	Modifying FortiGate administrator password to complex ones via SSH triggers a FortiManager password change by auto-update.
540634	Status of a port member of a redundant interface changes if an alias is set.
541211	Cannot create soft switch with VX LAN interface under same base interface.
541243	DHCP option doesn't include all NTP servers.
542258	DHCP exclusion isn't used for new DHCP range if the range is lower than the existing DHCP range.

Upgrade

Bug ID	Description
495994	After upgrade to V5.4.9, observing lot of IPS syntax errors on the console screen.
511529	`vdom-property` limits error after upgrade from 5.4.6 to 5.6.3.
524948	Wrong `management-vdom` after upgrade from V6.0 or rebooting FortiGate.
530793	`config-error-log` shows after upgrade from v5.6.6 to v5.6.7.

User & Device

Bug ID	Description
437117	Single Sign-on, multiple FSSO polling servers with the same AD (LDAP) server, cannot select the same user or group.
453095	Mobile FortiTokens not assignable VDOM in vcluster on slave unit.
470803	`fnbamd` uses high CPU when receive user member groups.
499941	Not able to SSH into FortiGate through FortiManager using TACAS+ user.
516403	FSSO - established session aren't re-evaluated when a user is removed from an Active Directory group.
523891	FortiGate: Unable to browse structure of Netscape LDAP.
525648	FortiOS does not prompt for token when Access-Challenge is received - RADIUS authentication fails.
525816	LDAP search issue after upgrade to 5.6.6 build 3444 from 5.6.5 build 3342.
525925	Unable to login to FortiGate using Symantec 2-factor authentication.

Bug ID	Description
525929	LDAPS requests fail with fnbamd stop error "Not enough bytes". LDAP works fine. Additional timeout observed.
527340	FortiGate fails to match User group after passing authentication (Local User).
529945	Local certificate content changes should be directly applied for the `admin-server-cert` sent to the client browser.
535279	FortiGate sends error user password to RADIUS server for CMCC auth user sometimes.
538304	Aggregate interface (four member) flapps when the third member interface goes down.
538407	FortiOS doesn't allow setting `source-ip` for mobile token activation.

VM

Bug ID	Description
484540	FOS VM serial number changes during firmware upgrade.
512019	FortiGate VM closed network + UTM license showing *Package update failed due to invalid contract*.
512713	Connectivity loss between FGT-SVM and FGT-VMX cause license to became invalid after one hour.
526471	VMX: Adding a security group with ~30+ devices into the redirection policy the connection starts to experience huge delay.
528405	FortiMeter Consumption is not accurate.
540062	Kernel panic after upgrade from 5.6.7 to 5.6.8.
541531	Service Manager is not automatically updated with the NSX dynamic security groups.

VoIP

Bug ID	Description
508277	Non-SIP packet send to SIP ALG got dropped with no log.
509625	Issues with RTP when ISP connections flaps when two equal default routes are present.

WCCP

Bug ID	Description
500087	Support WCCP set up with one arm WCCP web cache diagram.

Web Application Firewall

Bug ID	Description
463468	Clients are unable to connect to the mail server when WAF is enabled on the VIP policy.

Web Filter

Bug ID	Description
486087	Unable to open one URL on the redirection after the upgrade.
499604	Web Filter profile with SSL does not check SNI against server certificate.
499864	Web Filter profile's proxy options to allow corporate Gmail accounts gets overlooked if "general interest" category is blocked.
506707	Web filter CLI only `options` are unset when clicking *Apply* via GUI.
507253	`ovrd-auth-port-https` uses VIP's mapped IP as CN when no TLS SNI is present.
509860	Regex case insensitivity flag is ignored in 5.6.5 and 6.0.2 when FortiGate is in proxy mode.
526555	WAD Segmentation Signal 11 in 6.0.3.
531101	Web Filter inspection proxy mode unable to resolve hostname because website is unrated.
531471	The URL filter is not blocking a page when there are many entries in it.
532823	Wrong FortiGuard page displayed with Override enabled on Web Filter profile.
536099	"Filtering Services Availability" keeps showing as green even when port 8888 is blocked by an upstream device.
541539	URL filter wildcard expression not matched correctly in proxy mode.

WiFi Controller

Bug ID	Description
503106	Remote site client connected to the FAP14C Ethernet port is randomly not able to reach the LAN client connected to the FortiGate.
505661	FortiWiFi sends DHCP Offer as a unicast address via WiFi interface even though the BROADCAST bit is set to "1" in DHCP Discover.
507622	FortiGate does not send WTP-ID in RADIUS accounting packet when client is connected with captive-portal SSID.
512606	FortiWiFi not working with FortiPresence Pro.
519321	FWF-50E kernel panic due to a WiFi driver issue.
520521	Application hostapd crashed - causing a wireless outage.
521832	CAPWAP traffic is not offloaded successfully when using dynamic-vlan SSID and IPS profile or AV profile is enabled in the policy.

Bug ID	Description
522762	Frequent hostapd crash.
525959	Part of FAP221C and FAPC24JE went offline and failed to be managed by the controller again.
526107	Repeated `vfnb_netdev_event:1406 fix me!!!` after deleting WiFi DDIS from split VDOM.
527587	Different accounting behavior between FAP221C and FAPC24JE for CMCC portal auth.
530328	CAPWAP traffic dropped when offloaded if packets are fragmented.
543562	11r clients stuck on the default/fail VLAN when using WPA2 enterprise and dynamic-vlan while roaming between APs.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
395544	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2017-17544
452730	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2017-14186
496642	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13371
528040	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13384
529353	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13380
529377	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13379
529712	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13381
529719	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13383
529745	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2018-13382
534592	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2019-5587
539553	FortiOS 6.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2019-5586

Known Issues

The following issues have been identified in version 6.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.

Data Leak Prevention

Bug ID	Description
547437	WAD crash due to scheduler error occurs when oversized file is bypassing the DLP sensor.
548396	DLP archiving intermittently blocks a file when it should be log only.

Explicit Proxy

Bug ID	Description
548415	User cannot pass authentication after timeout if using IP-based authentication.

Firewall

Bug ID	Description
541348	Shaper in shaping policy is not applied when URL category is configured.

FortiView

Bug ID	Description
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
482045	FortiView – no data shown on *Traffic from WAN*.
526956	FortiView widgets get deleted upon upgrading to B222.
544017	FortiView > VPN 1 hour historical shows entries from 8 hours ago when logged in from FortiCloud.

GUI

Bug ID	Description
439185	AV quarantine cannot be viewed and downloaded from detail panel when source is FortiAnalyzer.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
451776	Admin GUI has limit of 10 characters for OTP.
504770	Introduce an enable/disable button in the GUI to toggle central SNAT table.
532309	Custom device page keep loading and cannot create device group.
546254	Forward traffic log cannot be shown on Windows Edge browser.
546953	DNS Filter column and Profile Group column is missing on policy list.
547393	GUI still shows `fortianalyzer-cloud` connection status error even after FortiGate connects to `fortianalyzer-cloud`.
547458	Cannot access VOIP profile list and only the default profile editor is shown.
547808	Security rating event logs cannot be shown in `split-vdom` FortiGate GUI.
548091	Cannot configure network interface IP addresses from GUI for FG-5001D and FG-5001E.

HA

Bug ID	Description
479987	FG MGMT1 does not authenticate Admin RADIUS users through primary unit (secondary unit works).

Intrusion Prevention

Bug ID	Description
445113	IPS engine 3.428 on FortiGate sometimes cannot detect Psiphon packets that iscan can detect.
548649	IPS custom signature is not detected after FortiGate is rebooted or upgraded.

IPsec VPN

Bug ID	Description
469798	The interface shaping with egress shaping profile doesn't work for offloaded traffic.
481201	The OCVPN feature is delayed about one day after registering on FortiCare.
545871	IPsec tunnel can't establish if OCVPN members with different Fortinet_CA and Fortinet_factory cert.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create web filter logs.

Proxy

Bug ID	Description
546360	When applying proxy address in transparent proxy policy, FortiGate blocks traffic and reports `SSL_ERROR_SYSCALL`.
548233	SMTP, POP3, IMAP `starttls` cannot be exempted by FortiGate when first time traffic goes through FortiGate.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.
547659	Access denied error when reviewing security recommendations from physical topology in VDOM mode.
547509	Fail to configure Security Fabric if only enable FortiAnalyzer cloud logging not FortiAnalyzer logging in GUI.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.
476838	Check domain log-on as SSL VPN host checks condition.
495522	RDP session freezes when using SSL VPN tunnel mode.

Switch Controller

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
462552	Add an extra dialog in the interface page to clean up config when changing a FortiLink interface back to a regular port.
548145	Configuring FortiLink from GUI does not work on platforms that do not support hardware switch.

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
385860	FG-3815D does not support 1GE SFP transceivers.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
472843	When FortiManager is set for `DM = set verify-install-disable`, FortiGate does not always save script changes.
474132	FG-51E hang under stress test since build 0050.
494042	If we create VLAN in VDOM A, then we cannot create ZONE name with the same VLAN name in VDOM B.
495532	EHP drop improvement for units with no NP_SERVICE_MODUL.
548076	FortiGateCloud cannot restore configuration on FortiGate.

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and web filter.
473075	When upgrading, multicast policies are lost when there is a zone member as interface.
481408	When upgrading from 5.6.3 to 6.0.0, the IPv6 policy is lost if there is SD-WAN member as interface.
494217	Peer user SSL VPN personal bookmarks do not show when upgrade to 6.0.1. **Workaround**: Use CLI to rename the user bookmark to the new name.
539112	Devices configured under `security-exempt-list` become void after upgrade.
548256	Upgrading to v6.2 from v6.0.x causes CIFS/SMB configurations in AV profile to be lost.
548813	Upgrading or downgrading the firmware image using FortiGuard as the source, and as initiated from the *System* > *Firmware* page, fails during download of the firmware image. The page still can be used to view the upgrade path, but as a workaround, you will need to manually download the firmware image from Fortinet's Support site, and then initiate an upgrade or downgrade from the same page under the *Upload Firmware* section.

VM

Bug ID	Description
548453	Ondemand platforms show error with FortiCare/FortinetOne login.

Bug ID	Description
548531	FGT-AWS HA failover and SDN using IAM role do not work due to AWS IAM role token length being +increased.

Web Filter

Bug ID	Description
538593	B0821: FGD service on https/8888 does not work well under specific wanopt topology.
544342	When `encryption` is set to yes, `file-type` incorrectly shows all file types when only `zip` files are supported.
544342	Web filter file: filter match only encrypted files will still block un-encrypted MS Office files.
545334	Web filter file filtering does not support FTP traffic inspection but user can still configure FTP protocol in GUI and CLI.
547772	Web filter FGD category is not detected by sniffer policy for HTTPS traffic.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.